

**Q66458**

Claims 1, 7, 11, 17, and 21

Cited literature: Japanese Unexamined Patent Application Publication 2000-235528

Remarks

Claims 1, 7, 11, 17, and 21

Cited Literature 1

Cited Literature 1 describes returning an electronically signed reception message (corresponding to the “certified response” of the present application) to the server relay unit (corresponding to the “first authentication means” of the present application) when the client relay unit (corresponding to the “second authentication means” of the present application) receives a message (corresponding to the “exchange message” of the present application), and also describes time-stamping the message. It is found that the client relay unit here stores messages from the server relay unit, as well as storing exchange messages between entities. Furthermore, since what volume of exchange messages is to be stored is something which can be suitably selected by a person skilled in the art, storing all exchange messages between entities is also something which could be easily thought of by a person skilled in the art. There cannot be said to be any remarkable technical difficulty in making the entity an electronic transaction entity or in stamping and storing messages.

## 拒絶理由通知書

特許出願の番号	特願2000-298939
起案日	平成17年 8月26日
特許庁審査官	永野 志保 3350 5500
特許出願人代理人	机 昌彦(外2名) 様
適用条文	第29条第2項

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から60日以内に意見書を提出して下さい。

## 理 由

この出願の下記の請求項に係る発明は、その出願前日本国内又は外国において頒布された下記の刊行物に記載された発明又は電気通信回線を通じて公衆に利用可能となった発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第29条第2項の規定により特許を受けることができない。

## 記

請求項 1, 7, 11, 17, 21

引用文献 特開2000-235528号公報

## 備考

請求項 1, 7, 11, 17, 21

引用文献 1

引用文献1には、クライアント中継部（本願の「第2の公証手段」に相当）が、メッセージ（本願の「交換メッセージ」に相当）を受信した際、サーバ中継部（本願の「第1の公証手段」に相当）に、電子署名を付加した受領メッセージ（本願の「証明応答」に相当）を返信することや、メッセージに時刻を打刻することも記載されており、クライアント中継部はサーバ中継部からのメッセージを記憶しており、エンティティ間の交換メッセージを記憶していると認められる。また、記憶する交換メッセージの量をどの程度にするかは当業者が適宜選択し得るものであるから、エンティティ間の全ての交換メッセージを記憶することも当業者が容易に思いつくことにすぎない。なお、エンティティを電子商取引エンティティとすることやメッセージに打刻して記憶することに格別な技術的困難性があるとはいえない。

拒絶の理由が新たに発見された場合には拒絶の理由が通知される。

#### 引 用 文 献 等 一 覧

補正では以下の点を注意されたい。

- (1) 明細書を補正した場合は、補正により記載を変更した個所に下線を引くこと。
- (2) 補正は、この出願の出願当初の明細書又は図面に記載した事項のほか、出願当初の明細書又は図面に記載した事項から自明な事項の範囲内で行わなければならない。補正の際には、意見書で、各補正事項について補正が適法なものである理由を、根拠となる出願当初の明細書等の記載箇所を明確に示したうえで主張されたい。
- (3) なお、上記の補正等の示唆は法律的效果を生じさせるものではなく、拒絶理由を解消するための一案である。明細書等をどのように補正するかは出願人が決定すべきものである。

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-235528

(43)Date of publication of application : 29.08.2000

(51)Int.Cl.

G06F 13/00

G06F 9/46

G06F 15/00

(21)Application number : 11-038026

(71)Applicant : FUJI XEROX CO LTD

(22)Date of filing : 17.02.1999

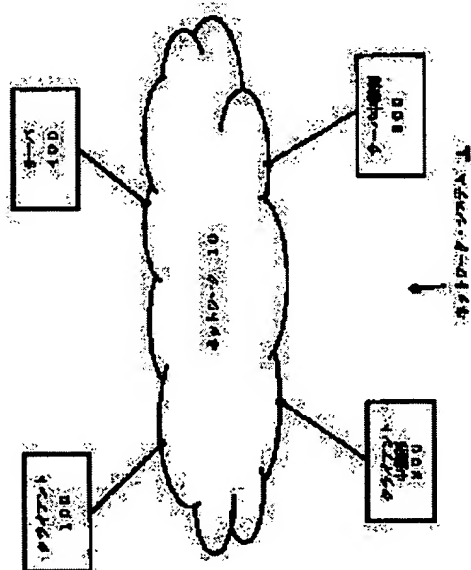
(72)Inventor : HORIKIRI KAZUNORI

## (54) METHOD FOR EXECUTING REMOTE PROCEDURE CALL ON NETWORK

(57)Abstract:

**PROBLEM TO BE SOLVED:** To obtain an excellent remote procedure call method capable of objectively certifying history information related to the execution of a remote procedure.

**SOLUTION:** Since a client repeating part 200 generates a 1st electronic signature corresponding to a request message and transmits the generated signature together with the request message, a server repeating part 300 can check the validity of the request message based on the 1st electronic signature. The server repeating part 300 generates a 2nd electronic signature corresponding to data synthesized from the request message and a response message and transmits the 2nd electronic signature together with the response message, so that the repeating part 200 can check the validity of the response message based on the 2nd signature. The repeating part 200 generates and transmits a 3rd electronic signature corresponding to data synthesized from the request message and the response message, so that the repeating part 300 can check the reception of the response message.



## LEGAL STATUS

[Date of request for examination] 12.03.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's]

decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-235528

(P2000-235528A)

(43) 公開日 平成12年8月29日 (2000.8.29)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 F 5 B 0 8 5
9/46	3 6 0	9/46	3 6 0 B 5 B 0 8 9
15/00	3 3 0	15/00	3 3 0 A 5 B 0 9 8

審査請求 未請求 請求項の数10 O L (全 12 頁)

(21) 出願番号 特願平11-38026

(22) 出願日 平成11年2月17日 (1999.2.17)

(71) 出願人 000005496

富士ゼロックス株式会社

東京都港区赤坂二丁目17番22号

(72) 発明者 堀切 和典

神奈川県足柄上郡中井町境430グリーンテ

クなかい 富士ゼロックス株式会社

(74) 代理人 100086531

弁理士 澤田 俊夫

F ターム (参考) 5B085 AED0 BG07

5B089 GA11 GA21 HB04 HB05 JA00

JA11 JB03 KA13 MC03

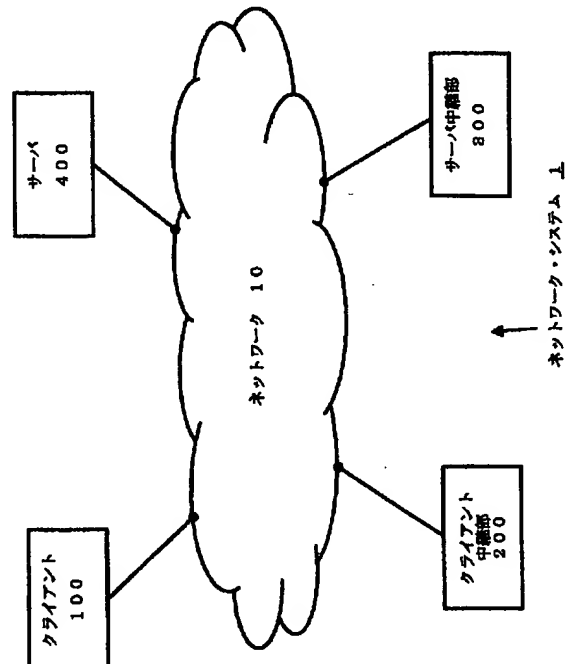
5B098 AA10 GC16 JJ07

(54) 【発明の名称】 ネットワーク上において遠隔手続き呼び出しを実行するための方法

(57) 【要約】

【課題】 遠隔手続きの実行に関する履歴情報を客観的に証明することができる、優れた遠隔手続き呼び出し方式を提供する。

【解決手段】 クライアント中継部は、要求メッセージに対する第1の電子署名を生成して要求メッセージとともに送信するので、サーバ中継部では、第1の電子署名を元に要求メッセージの正当性を検査することができる。サーバ中継部は、要求メッセージと応答メッセージを合成したデータに対する第2の電子署名を生成して応答メッセージとともに送信するので、クライアント中継部では、第2の電子署名を元に応答メッセージの正当性を検査することができる。クライアント中継部は、要求メッセージと応答メッセージを合成したデータに対する第3の電子署名を生成して送信するので、サーバ中継部では応答メッセージの受信を確認することができる。



## 【特許請求の範囲】

【請求項 1】 サービスを要求する 1 以上のクライアントとサービス・オブジェクトを有する 1 以上のサーバとで構成されるネットワーク上において遠隔手続き呼び出しを実行するための方法であって、(a) クライアントが、遠隔手続き呼び出し方式の要求メッセージについての第 1 の電子署名を生成する段階と、(b) クライアントが、要求メッセージを第 1 の電子署名とともに送信する段階と、(c) サーバが、受信した要求メッセージに添付された第 1 の電子署名を検査する段階と、(d) サーバが、要求メッセージに対する応答メッセージを生成する段階と、(e) サーバが、要求メッセージと応答メッセージから合成されるデータに対して第 2 の電子署名を生成する段階と、(f) サーバが、応答メッセージを第 2 の電子署名とともに送信する段階と、(g) クライアントが、受信した応答メッセージの正当性を、第 2 の電子署名を元に検査する段階と、(h) クライアントが、少なくとも要求メッセージと応答メッセージから合成されたデータに対して第 3 の電子署名を生成する段階と、(i) クライアントが、サーバに第 3 の電子署名を送信する段階と、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項 2】 (p) サーバが、受信した要求メッセージと第 1 の電子署名を格納する段階、(q) サーバが、第 3 の電子署名を格納する段階、(r) クライアントが、第 2 の電子署名を格納する段階、のうち少なくとも 1 つを含むことを特徴とする請求項 1 に記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項 3】 サービスを要求する 1 以上のクライアントとサービス・オブジェクトを有する 1 以上のサーバとで構成されるネットワーク上において、クライアント中継部とサーバ中継部の介在により遠隔手続き呼び出しを実行するための方法であって、(a) クライアントが、遠隔手続き呼び出し方式の要求メッセージをクライアント中継部に送信する段階と、(b) クライアント中継部が、要求メッセージに対して第 1 の電子署名を生成する段階と、(c) クライアント中継部が、サーバ中継部に対して、要求メッセージを第 1 の電子署名とともに送信する段階と、(d) サーバ中継部が、第 1 の電子署名を元に受信した要求メッセージを検査する段階と、(e) サーバ中継部が、サーバに要求メッセージを送信する段階と、(f) サーバが、要求メッセージに対する応答メッセージを生成する段階と、(g) サーバが、応答メッセージをサーバ中継部に送信する段階と、(h) サーバ中継部が、要求メッセージと応答メッセージとから合成されるデータに対して第 2 の電子署名を生成する段階と、(j) サーバ中継部が、応答メッセージを第 2 の電子署名とともに送信する段階と、(k) クライアント中継部が、受信した応答メッセージの正当性を、第 2 の電子署名を元に検査する段階と、(l) クライアント中継

部が、少なくとも要求メッセージと応答メッセージから合成されたデータに対して第 3 の電子署名を生成する段階と、(m) クライアント中継部が、サーバ中継部に第 3 の電子署名を送信する段階と、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項 4】 (p) サーバ中継部が、受信した要求メッセージと第 1 の電子署名を格納する段階、(q) サーバ中継部が、第 3 の電子署名を格納する段階、(r) クライアント中継部が、第 2 の電子署名を格納する段階、のうち少なくとも 1 つを含むことを特徴とする請求項 3 に記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項 5】 遠隔手続き呼び出しを実行可能なネットワーク・システムであって、

遠隔手続き呼び出し方式の要求メッセージを生成するクライアントと、

要求メッセージに対する応答メッセージを生成するサーバと、

クライアントが要求メッセージを発行したこと及びクライアントがサーバからの応答メッセージを受信したことを客観的に証明するクライアント中継部と、

サーバが要求メッセージに対する応答メッセージを生成したことを客観的に証明するサーバ中継部と、を具備することを特徴とする遠隔手続きを実行可能なネットワーク・システム。

【請求項 6】 サービスを要求する 1 以上のクライアントとサービス・オブジェクトを有する 1 以上のサーバとで構成されるネットワーク上において、クライアントとサーバ間の遠隔手続き呼び出し実行のために介在するクライアント中継部であって、

クライアントから要求メッセージを受信する手段と、

クライアントが生成した要求メッセージに対して第 1 の電子署名を生成する手段と、

第 1 の電子署名付きで要求メッセージを送信する手段と、

第 2 の電子署名付きで応答メッセージを受信する手段と、

第 2 の電子署名を元に受信した応答メッセージを検査する手段と、

要求メッセージと応答メッセージから合成されたデータに対して第 3 の電子署名を生成する手段と、

第 3 の電子署名を送信する手段と、

を含むことを特徴とするクライアント中継部。

【請求項 7】 さらに、第 2 の電子署名を記憶する手段を含むことを特徴とする請求項 6 に記載のクライアント中継部。

【請求項 8】 さらに、応答メッセージを記憶する手段を含むことを特徴とする請求項 6 に記載のクライアント中継部。

## 3

【請求項 9】サービスを要求する 1 以上のクライアントとサービス・オブジェクトを有する 1 以上のサーバとで構成されるネットワーク上において、クライアントとサーバ間の遠隔手続き呼び出し実行のために介在するサーバ中継部であって、

第 1 の電子署名付きで要求メッセージを受信する手段と、

第 1 の電子署名を元に要求メッセージを検査する手段と、

サーバに要求メッセージを送信する手段と、

サーバから応答メッセージを受信する手段と、

要求メッセージと応答メッセージから合成されたデータに対して第 2 の電子署名を生成する手段と、

第 2 の電子署名付きで応答メッセージを送信する手段と、

第 3 の電子署名を受信する手段と、を含むことを特徴とするサーバ中継部。

【請求項 10】さらに、要求メッセージと第 1 の電子署名、及び、第 3 の電子署名を記憶する手段を含むことを特徴とする請求項 9 に記載のサーバ中継部。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、1 以上のサーバと 1 以上のクライアントからなる分散環境のネットワーク・システムにおいてクライアントがサーバに対してサービスを要求するための遠隔手続き呼び出し方式に係り、特に、遠隔手続きの実行に関する履歴情報を客観的に証明するための遠隔手続き呼び出し方式に関する。

【0002】更に詳しくは、本発明は、クライアントがサービス要求を行なったこと、サーバがサービス要求に対して応答したこと、クライアントがサーバからのサービス応答を受け取ったことを客観的に証明するための遠隔手続き呼び出し方式に関する。

【0003】

【従来の技術】昨今の情報処理・情報通信の分野における発展は目覚ましいものがある。この種の技術分野においては、コンピュータ・システム同士を相互接続するための研究・開発が、以前から活発になされてきた。システム同士を相互接続する主な目的は、複数ユーザによるコンピュータ資源の共有や、情報の共有・流通などである。

【0004】システム間を接続するための伝送媒体すなわち「ネットワーク」としては、大学や事業所の構内など限られた空間内に敷設された LAN (Local Area Network) の他、LAN を専用回線で接続した WAN (Wide Area Network) や、一般公衆回線 (PSTN)、ISDN (Integrated Service Digital Network)、インターネットなど様々である。

【0005】ネットワーク・システムは、一般に、ネッ

## 4

トワーク上の特定のコンピュータをサーバ (ファイル・サーバ、プリント・サーバ) とし、これを他のクライアントが利用し合うというクライアント・サーバ型として構築される。

【0006】かかるクライアント・サーバ型モデルにおいては、クライアント側のプログラムを構成する一部の手続きの実行をネットワーク上の別のコンピュータに委託するというメカニズム、すなわち「遠隔手続き呼び出し (RPC: Remote Procedure Call)」、若しくは「遠隔メソッド呼び出し (RMI: Remote Method Invocation)」が用いられる。遠隔手続きの実行結果は、戻り値として、呼び出した側のコンピュータに返される。また、手許のコンピュータのキーボードやファイルを使ってプログラムへの入力を果たしたり、同じコンピュータのディスプレイやファイルに出力することもできる。

【0007】遠隔手続き若しくは遠隔メソッド呼び出しの仕組みは、LAN の世界に限定されず、さらに、インターネットのような広域的なネットワーク上でも利用可能である。

【0008】例えば、インターネット上には、WWW (World Wide Web) と呼ばれる、ハイパーリンク構造の資源空間を提供する広域情報検索システムが公開されている。この WWW 資源空間上では、HTTP (Hyper Text Transfer Protocol) の他、HTTPS、S-HTTP (secure HTTP)、FTP (File Transfer Protocol)、CORBA (Common ORB Architecture)、IIOP (Internet Inter-ORB Protocol)、JavaRMI (Remote Method Invocation) などの各種プロトコルに従って WWW サーバと WWW クライアント間でメッセージ交換が行なわれるが、これらは遠隔手続き／遠隔メソッド呼び出しの形態で実現される。このうち HTTP プロトコルについては、例えば RFC (Request For Comments) 1945 や RFC 2068 に記述されている。

【0009】WWW 上で特によく利用されるサービス資源は、HTML (Hyper Text Markup Language) という言語で記述された文書、すなわちハイパーテキストである。HTML については、例えば RFC 1866 に記述されている。

【0010】また、WWW サーバが所有する各資源は、URL (Uniform Resource Locator) という形式の識別子によって特定される。URL とは、資源の名前とを指定した文字列であり、「スキーム名 (プロトコル名) : // ホスト名 (ドメイン名) : ポート番号 / パス名 (ファイル名)」という形式で記述される。URL については、例えば RFC 173



8やRFC1808などに記述されている。ここで言うホスト名は、TCP/IP (Transmission Control Protocol/Internet Protocol) ネットワークで用いられるネーム・サービスであるDNS (Domain Name System) の体系に従う。DNSでは、ドメインと呼ぶ論理的なグループを階層的に設定することができ、その論理グループの名称であるドメイン名をコンピュータの名前(ホスト名)の一部に組み込んで利用される。DNSサーバは、ドメイン名とIPアドレスの対応表を持

っており、ドメイン名に基づく問い合わせに対して該当するIPアドレスを返すようになっている(周知)。  
 【0011】ところで、旧来型のクライアント・サーバ・アプリケーションの構成では、クライアントとサーバが同一組織内のLANを経由して接続される方式が採用される。このような場合、クライアント側が呼び出した遠隔手続き呼び出しの実行処理は、通常、課金や計数の対象とはならない。これに対し、アプリケーションを構成するクライアントとサーバが異なる組織や団体で運営されているような場合、遠隔手続きを呼び出したクライアント(又はクライアントが属する組織)は、該手続きを実行したサーバ(又はサーバが属する組織)に対して、呼び出された手続きの実行に対する対価を支払う義務を負うと考えるのが相当であろう。特に、最近のネットワーク環境では、互いに異なる組織又は団体に帰属するクライアントとサーバとがインターネットのような外部ネットワークを介して接続されているので、後者のケースが非常に多くなってきている。

【0012】ところが、呼び出された手続きの実行したという事実を、下記のように客観的に証明するような遠隔手続き呼出方式や装置は存在しない。

(1) クライアントがサービス要求したことを、後日客観的に証明できる。

(2) 要求されたサービスに対してサーバが応答したことを、後日客観的に証明できる。

(3) サーバによるサービス応答をクライアントが受信したことを、後日客観的に証明できる。

【0013】例えば、特開平10-313308号公報には、ホームページ作成者の公開鍵証明書とホームページの固有情報への署名をサーバからクライアントにダウンロードして、クライアント側で署名検証処理を行う「ホームページ認証方法及び装置」について開示している。同公報によれば、1つのサーバに複数のホームページがあり、ホームページ毎に管理者が異なる場合であっても、サーバ単位ではなく、ホームページ単位でページ作成者の認証処理が可能となる。しかしながら、同公報によっても、クライアントがサーバに対して要求メッセージを送信したことや、クライアントがサーバからの応答メッセージを受信したことを、客観的に証明できる仕組みや機構については一切言及していない。

【0014】また、特開平10-171887号公報には、電子マネーを利用して取引する場合に、取引内容や決済が完了したことを客観的に証明できる電子データをオープンなネットワーク上で提供したオンラインショッピングシステムについて開示している。しかしながら、同公報に開示されたシステムでは、サーバがクライアントにサービスを提供する場合、クライアントが送信した要求メッセージをサーバが受信したことや、サーバが送信した応答メッセージをクライアントが受信したことなどを、客観的に証明するための仕組みや機構については全く言及していない。

【0015】

【発明が解決しようとする課題】本発明の目的は、1以上のサーバと1以上のクライアントからなる分散環境のネットワーク・システムにおいてクライアントがサーバに対してサービスを要求する、優れた遠隔手続き呼び出し方式を提供することにある。

【0016】本発明の更なる目的は、遠隔手続きの実行に関する履歴情報を客観的に証明することができる、優れた遠隔手続き呼び出し方式を提供することにある。

【0017】本発明の更なる目的は、クライアントがサービス要求を行なったこと、サーバがサービス要求に対して応答したこと、クライアントがサーバからのサービス応答を受け取ったことを客観的に証明することができる、優れた遠隔手続き呼び出し方式を提供することにある。

【0018】

【課題を解決するための手段及び作用】本発明は、上記課題を参酌してなされたものであり、その第1の側面は、サービスを要求する1以上のクライアントとサービス・オブジェクトを有する1以上のサーバとで構成されるネットワーク上において遠隔手続き呼び出しを実行するための方法であって、(a)クライアントが、遠隔手続き呼び出し方式の要求メッセージについての第1の電子署名を生成する段階と、(b)クライアントが、要求メッセージを第1の電子署名とともに送信する段階と、(c)サーバが、受信した要求メッセージに添付された第1の電子署名を検査する段階と、(d)サーバが、要求メッセージに対する応答メッセージを生成する段階と、(e)サーバが、要求メッセージと応答メッセージから合成されるデータに対して第2の電子署名を生成する段階と、(f)サーバが、応答メッセージを第2の電子署名とともに送信する段階と、(g)クライアントが、受信した応答メッセージの正当性を、第2の電子署名を元に検査する段階と、(h)クライアントが、少なくとも要求メッセージと応答メッセージから合成されたデータに対して第3の電子署名を生成する段階と、

(i)クライアントが、サーバに第3の電子署名を送信する段階と、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法である。

【0019】第1の側面に係るネットワーク上で遠隔手続き呼び出しを実行するための方法において、さらに、  
 (p) サーバが、受信した要求メッセージと第1の電子署名を格納する段階、(q) サーバが、第3の電子署名を格納する段階、(r) クライアントが、第2の電子署名を格納する段階、のうち少なくとも1つを含んでいてもよい。

【0020】クライアントは、要求メッセージに対する第1の電子署名を生成し、且つ、第1の電子署名を添付して要求メッセージを送信するので、これを受け取ったサーバ側では、要求メッセージの正当性を検査したり確認することができる。また、サーバは、受信した要求メッセージと第1の電子署名を格納することによって、特定のクライアントから要求メッセージを受け取ったという事実を、後日客観的に証明することができる。

【0021】また、サーバは、要求メッセージと応答メッセージを合成したデータに対する第2の電子署名を生成し、且つ、第2の電子署名を添付して応答メッセージを送信するので、これを受け取ったクライアント側では、応答メッセージの正当性を検査したり確認することができる。また、クライアントは、第2の電子署名を格納することによって、サーバから受け取った応答メッセージの内容を、後日客観的に証明することができる(例えば、不良な応答メッセージを戻されたという事実を証明することができる)。

【0022】また、クライアントは、要求メッセージと応答メッセージを合成したデータに対する第3の電子署名を生成して送信するので、これを受け取ったサーバ側では、クライアントが応答メッセージを受け取ったことを確認することができる。また、サーバは、受信した第3の電子署名を格納することによって、クライアントに対して応答メッセージを送信したという事実を、後日客観的に証明することができる。

【0023】また、本発明の第2の側面は、サービスを要求する1以上のクライアントとサービス・オブジェクトを有する1以上のサーバとで構成されるネットワーク上において、クライアント中継部とサーバ中継部の介在により遠隔手続き呼び出しを実行するための方法であって、(a) クライアントが、遠隔手続き呼び出し方式の要求メッセージをクライアント中継部に送信する段階と、(b) クライアント中継部が、要求メッセージに対して第1の電子署名を生成する段階と、(c) クライアント中継部が、サーバ中継部に対して、要求メッセージを第1の電子署名とともに送信する段階と、(d) サーバ中継部が、第1の電子署名を元に受信した要求メッセージを検査する段階と、(e) サーバ中継部が、サーバに要求メッセージを送信する段階と、(f) サーバが、要求メッセージに対する応答メッセージを生成する段階と、(g) サーバが、応答メッセージをサーバ中継部に送信する段階と、(h) サーバ中継部が、要求メッセー

ジと応答メッセージとから合成されるデータに対して第2の電子署名を生成する段階と、(j) サーバ中継部が、応答メッセージを第2の電子署名とともに送信する段階と、(k) クライアント中継部が、受信した応答メッセージの正当性を、第2の電子署名を元に検査する段階と、(l) クライアント中継部が、少なくとも要求メッセージと応答メッセージから合成されたデータに対して第3の電子署名を生成する段階と、(m) クライアント中継部が、サーバ中継部に第3の電子署名を送信する段階と、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法である。

【0024】ここで、第2の側面に係るネットワーク上で遠隔手続き呼び出しを実行するための方法において、さらに、(p) サーバ中継部が、受信した要求メッセージと第1の電子署名を格納する段階、(q) サーバ中継部が、第3の電子署名を格納する段階、(r) クライアント中継部が、第2の電子署名を格納する段階、のうち少なくとも1つを含んでいてもよい。

【0025】クライアント中継部は、要求メッセージに対する第1の電子署名を生成し、且つ、第1の電子署名を添付して要求メッセージを送信するので、これを受け取ったサーバ中継部では、要求メッセージの正当性を検査したり確認することができる。また、サーバ中継部は、受信した要求メッセージと第1の電子署名を格納することによって、特定のクライアントからの要求メッセージを受け取ったという事実を、後日客観的に証明することができる。

【0026】また、サーバ中継部は、要求メッセージと応答メッセージを合成したデータに対する第2の電子署名を生成し、且つ、第2の電子署名を添付して応答メッセージを送信するので、これを受け取ったクライアント中継部では、応答メッセージの正当性を検査したり確認することができる。また、クライアント中継部は、第2の電子署名を格納することによって、サーバが生成した応答メッセージの内容を、後日客観的に証明することができる(例えば、不良な応答メッセージを戻されたという事実を証明することができる)。

【0027】また、クライアント中継部は、要求メッセージと応答メッセージを合成したデータに対する第3の電子署名を生成して送信するので、これを受け取ったサーバ中継部では、クライアント中継部(または、クライアント)が応答メッセージを受け取ったことを確認することができる。また、サーバ中継部は、受信した第3の電子署名を格納することによって、クライアントに対して応答メッセージを送信したという事実を、後日客観的に証明することができる。

【0028】また、本発明の第3の側面は、遠隔手続きを実行可能なネットワーク・システムであって、遠隔手続き呼び出し方式の要求メッセージを生成するクライアントと、要求メッセージに対する応答メッセージを生成

10

20

30

40

50

するサーバと、クライアントが要求メッセージを発行したこと及びクライアントがサーバからの応答メッセージを受信したことを客観的に証明するクライアント中継部と、サーバが要求メッセージに対する応答メッセージを生成したことを客観的に証明するサーバ中継部と、を具備することを特徴とする遠隔手続きを実行可能なネットワーク・システムである。

【0029】本発明の第3の側面に係るネットワーク・システムによれば、クライアントが要求メッセージを発行したことや、クライアントがサーバからの応答メッセージを受信したことなどの事実を、クライアント中継部が客観的に証明することができる。また、サーバが要求メッセージに対する応答メッセージを生成したことを、サーバ中継部が客観的に証明することができる。

【0030】また、本発明の第4の側面は、サービスを要求する1以上のクライアントとサービス・オブジェクトを有する1以上のサーバとで構成されるネットワーク上において、クライアントとサーバ間の遠隔手続き呼び出し実行のために介在するクライアント中継部であって、クライアントから要求メッセージを受信する手段と、クライアントが生成した要求メッセージに対して第1の電子署名を生成する手段と、第1の電子署名付きで要求メッセージを送信する手段と、第2の電子署名付きで応答メッセージを受信する手段と、第2の電子署名を元に受信した応答メッセージを検査する手段と、要求メッセージと応答メッセージから合成されたデータに対して第3の電子署名を生成する手段と、第3の電子署名を送信する手段と、を含むことを特徴とするクライアント中継部である。

【0031】クライアント中継部は、さらに、第2の電子署名を記憶する手段や、応答メッセージを記憶する手段を含んでいてもよい。

【0032】本発明の第4の側面に係るクライアント中継部は、要求メッセージに対する第1の電子署名を生成し、且つ、第1の電子署名を添付して要求メッセージを送信するので、これを受け取ったサーバ中継部やサーバでは、要求メッセージの正当性を検査したり確認することができる。また、サーバ中継部やサーバは、受信した要求メッセージと第1の電子署名を格納することによって、特定のクライアントからの要求メッセージを受け取ったという事実を、後日客観的に証明することができる。

【0033】また、クライアント中継部は、要求メッセージと応答メッセージを合成したデータに対する第3の電子署名を生成して送信するので、これを受け取ったサーバ中継部やサーバでは、クライアント中継部（または、クライアント）が応答メッセージを受け取ったことを確認することができる。また、サーバ中継部やサーバは、受信した第3の電子署名を格納することによって、クライアントに対して応答メッセージを送信したという

事実を、後日客観的に証明することができる。

【0034】また、本発明の第5の側面は、サービスを要求する1以上のクライアントとサービス・オブジェクトを有する1以上のサーバとで構成されるネットワーク上において、クライアントとサーバ間の遠隔手続き呼び出し実行のために介在するサーバ中継部であって、第1の電子署名付きで要求メッセージを受信する手段と、第1の電子署名を元に要求メッセージを検査する手段と、サーバに要求メッセージを送信する手段と、サーバから応答メッセージを受信する手段と、要求メッセージと応答メッセージから合成されたデータに対して第2の電子署名を生成する手段と、第2の電子署名付きで応答メッセージを送信する手段と、第3の電子署名を受信する手段と、を含むことを特徴とするサーバ中継部である。

【0035】サーバ中継部は、さらに、要求メッセージと第1の電子署名、及び、第3の電子署名を記憶する手段を含んでいてもよい。

【0036】本発明の第5の側面に係るサーバ中継部は、要求メッセージと応答メッセージを合成したデータに対する第2の電子署名を生成し、且つ、第2の電子署名を添付して応答メッセージを送信するので、これを受け取ったクライアント中継部やクライアントでは、応答メッセージの正当性を検査したり確認することができる。また、クライアント中継部やクライアントは、第2の電子署名を格納することによって、サーバが生成した応答メッセージの内容を、後日客観的に証明することができる（例えば、不良な応答メッセージを戻されたという事実を証明することができる）。

【0037】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0038】

【発明の実施の形態】以下、図面を参照しながら本発明の実施例を詳解する。

【0039】図1には、本発明の実施に供されるネットワーク・システム1の構成を模式的に示している。ネットワーク・システム1は、データ（すなわちサービス要求メッセージやサービス応答メッセージなど）の伝送媒体であるネットワーク10上に無数のデータ通信端末が接続されており、分散コンピューティング環境を提供している。以下、各部について説明する。

【0040】ネットワーク10は、例えば大学や企業の構内などの限られた空間内に敷設されたLAN（Local Area Network）である。あるいは、LAN同士を専用線等で相互接続してなるWAN（Wide Area Network）や、一般公衆回線（PSTN: Public Switched Telephone Network）、ISDN（Integrated Service Digital Network）、これらネットワークの大規模な集合体で

あるインターネットであってもよい。各データ通信端末は、モデムやTA(Terminal Adapter)、LANアダプタ等を介してネットワーク10に接続される。各データ通信端末同士は、ネットワーク10を介して、例えばTCP/IP(Transmission Control Protocol/Internet Protocol)接続されている。

【0041】本実施例のネットワーク・システム1は、ネットワーク10上の一部のデータ通信端末をサーバ400とし、サーバ400が提供するサービス資源を他の1以上のクライアント100…が利用し合うという、分散環境のクライアントーサーバ型モデルとして構築されている。

【0042】さらに、ネットワーク10上には、クライアント中継部200、及び、サーバ中継部300が接続されている。これら中継部200及び300は、分散環境下でのクライアント100及びサーバ400間のメッセージ送受信において、電子署名を利用したメッセージの正当性の検査や確認を行ない、さらに送受信の記録をとり、後日客観的に証明したりする。各中継部200及び300の構成や処理動作については、後に詳解する。

【0043】ネットワーク10に接続された各データ通信端末は、サーバ或いはクライアントとしてデザインされた専用のマシンであってもよいが、多くの場合は、サーバ用、クライアント用、サーバ中継用、クライアント中継用の各アプリケーションを導入して動作する汎用のコンピュータ・システム(ワークステーションやパーソナル・コンピュータ等)である。

【0044】サーバ400は、複数のサービス資源を所有している。クライアント100は要求メッセージを送信してサービス資源の提供を要求し、これに対して、サーバ400は応答メッセージという形式でサービス資源を提供する。

【0045】例えば、ネットワーク10上に構築されたクライアントーサーバ型モデルがWWW(World Wide Web)であれば、HTTP(Hyper Text Transfer Protocol)プロトコルに従ってメッセージがネットワーク10上を伝送する。この場合、サーバ400が所有するサービス資源は、例えばホームページを形成するためのHTML(Hyper Text Markup Language)ファイルである。また、クライアント100は、サーバのドメイン名を含んだURL(Uniform Resource Locator)の形式に従ってサービス資源を指定することができる(上述)。HTTPに従ったサービス要求メッセージは、一種の遠隔手続き/メソッド呼び出しである。

【0046】また、図2には、本発明の他の実施例に係るネットワーク・システム1の構成を模式的に示している。図1に係るネットワーク・システム1との相違は、

クライアント中継部200及びサーバ中継部300の各々は、ネットワーク10上で、独立したデータ通信端末としては存在せず、夫々、クライアント100及びサーバ400を構成する各コンピュータ・システム上で動作するクライアント中継用アプリケーション、サーバ中継用アプリケーションという形態で実装されている点である。図2に示す実施例の場合、クライアント100とクライアント中継部200の間、及びサーバ400とサーバ中継部300の間は、所定のプログラミング・インターフェースを介して接続されており、クライアント100とクライアント中継部200の間、及びサーバ400とサーバ中継部300の間がネットワーク接続されている図1に示す実施例とは相違する。

【0047】クライアント中継部200及びサーバ中継部300の主業務は、分散環境下でのクライアント100及びサーバ400間のメッセージ送受信において、電子署名を利用したメッセージの正当性の検査や確認を行なうこと、さらに、送受信の記録をとり、後日客観的に証明することにある。図1及び図2のいずれの実施形態であっても、クライアント中継部200及びサーバ中継部300の各々において遂行される動作は本質的に同一である。以下の説明では、ネットワーク・システム1が図1又は図2のいずれであるかを区別しないこととする。

【0048】なお、各中継部200及び300における電子署名方式として、例えば公開鍵暗号方式/\*/\*を採用することができる。

【0049】図3には、クライアント中継部200の構成を模式的に示している。クライアント中継部200は、要求署名生成部210と、記録部220と、送受信部230と、受領書生成部240と、応答メッセージ解析部250とで構成される。クライアント中継部200の実体は、ネットワーク10上の独立したデータ通信端末であっても、クライアント100と同じコンピュータ・システム上で動作するクライアント中継用アプリケーションであってもよい。

【0050】送受信部230は、ネットワーク10経由でのメッセージ送受信を行なう。送受信部230が扱うメッセージは、例えば、クライアント100から受け取る要求メッセージや、サーバ中継部300から受け取る応答メッセージ、応答メッセージに対する受領メッセージ(後述)などである。

【0051】記録部220は、要求署名生成部210、応答メッセージ解析部250、及び、受領書生成部240の各々からデータを受け取って、その保存を行なう。記録部220の実体は、例えば、クライアント中継部200を構成するコンピュータ・システムにローカル接続されたハード・ディスク装置のような補助記憶装置である。

【0052】要求署名生成部210は、クライアント1

10

20

30

40

50

00から受信した要求メッセージを要求先のサーバ400に向けて転送するに際し、第1の電子署名signature1を作成するための機能モジュールである。本実施例では、クライアント中継部200は公開鍵暗号系の秘密鍵secretkey1を保持している。要求署名生成部210は、要求メッセージに対してこの秘密鍵secretkey1で電子署名を行なうようになっている。より具体的には、メッセージ中で要求されているパラメータに対して、要求番号と現在時刻と有効期限を表すビット列を連結して、秘密鍵secretkey1

【0053】応答メッセージ解析部250は、サーバ中継部300から受信した応答メッセージを解析し検査するための機能モジュールである。本実施例では、応答メッセージ解析部250は、サーバ中継部300の公開鍵publickey2を保持しており、受信したメッセージを解析し、この公開鍵publickey2を用いて応答メッセージ中の第2の電子署名signature2を検証する。また、応答メッセージ解析部250

【0054】なお、応答メッセージ解析部250は、サーバ中継部300の公開鍵publickey2の代わりに、ネットワーク10で介在する認証局（図示しない）の公開鍵、又は、サーバ中継部300の公開鍵と認証局の公開鍵の双方を用いてもよい。

【0055】受領書作成部240は、サーバ中継部300から応答メッセージを受信したことに応答して、その受領書を発行するための機能モジュールである。本実施例では、クライアント中継部100は公開鍵暗号系の秘密鍵secretkey1を保持している。受領書作成部230は、応答メッセージ解析部250の出力に応じて、少なくとも要求メッセージ中のパラメータと応答メッセージから得られるメッセージ・ダイジェスト（後述）に対して秘密鍵secretkey1を用いて第3の電子署名signature3を作成し、これを受領メッセージとして送受信部230に出力する。

【0056】なお、クライアント中継部200には、DNSサーバ（Domain Name Service：上述）によって、ホスト名“client200”が与えられているものとする。

【0057】図4には、サーバ中継部300の構成を模式的に示している。サーバ中継部300は、応答署名生成部310と、記録部320と、送受信部330と、受領書解析部340と、要求メッセージ解析部250とで構成される。サーバ中継部300の実体は、ネットワーク10上の独立したデータ通信端末であっても、サーバ400と同じコンピュータ・システム上で動作するサーバ中継用アプリケーションであってもよい。

【0058】送受信部330は、ネットワーク10経由でのメッセージ送受信を行なう。送受信部330が扱うメッセージは、例えば、クライアント中継部200から受け取る要求メッセージや受領メッセージ、サーバ400から受け取る応答メッセージなどである。

【0059】記録部320は、応答署名生成部310、要求メッセージ解析部350、及び、受領書解析部340の各々からデータを受け取ってその保存を行なう。記録部320の実体は、例えば、サーバ中継部300を構成するコンピュータ・システムにローカル接続されたハード・ディスク装置のような補助記憶装置である。

【0060】応答署名生成部310は、サーバ400から受信した応答メッセージを要求元のクライアント100に向けて転送するに際し、第2の電子署名signature2を作成するための機能モジュールである。本実施例では、公開鍵暗号系の秘密鍵secretkey2を保持している。応答署名生成部310は、応答メッセージに対してこの秘密鍵secretkey2で第2の電子署名を行ない、応答メッセージとして送受信部330に出力する。

【0061】要求メッセージ解析部350は、クライアント中継部200から受信した要求メッセージを解析し検査するための機能モジュールである。本実施例では、クライアント中継部200の公開鍵publickey1を保持している。要求メッセージ解析部350は、受信したメッセージを解析し、この公開鍵publickey1を用いて要求メッセージ中の第1の電子署名signature1を検証する。また、要求メッセージ解析部350は、この第1の電子署名signature1を記録部320に転送して、これを保存する。

【0062】受領書解析部340は、送受信部330を介して受け取った受領メッセージを解析するための機能モジュールであり、クライアント中継部200の公開鍵publickey1を用いて受領メッセージ中の第3の電子署名signature3を検証する。また、要求メッセージ解析部350は、この第3の電子署名signature3を記録部320に転送して、これを保存する。

【0063】なお、サーバ中継部300には、DNSサーバ（上述）によって、ホスト名“server300”が与えられているものとする。

【0064】次に、クライアント中継部200及びサーバ中継部300を介して実現される、クライアント100及びサーバ400間のメッセージ送受信の動作手順について詳解する。

【0065】以下では、HTTPプロトコルを用いて、クライアント100がクライアント中継部200に第1の要求メッセージを送信し、クライアント中継部200がサーバ中継部300に第2の要求メッセージを送信し、サーバ中継部300がサーバ400に第3の要求メ

10

20

30

40

50

ッセージを送信する場合を例にとって説明する。但し、通信プロトコルはHTTPのみに限定されず、クライアント100、クライアント中継部200、サーバ中継部300、及び、サーバ400の各々は、HTTPS、S-HTTP、FTP、CORBA、IIOP、Java RMI、TCP、UDP (User Datagram Protocol) などの任意の通信プロトコルを使用してもよい。

【0066】まず、クライアント100は、[数1]に示すような第1の要求メッセージを生成し、クライアント中継部200に送信する。

【0067】

【数1】

GET /service?a=1 HTTP/1.1

【0068】クライアント中継部200では、送受信部230が第1の要求メッセージを受信すると、これを要求署名生成部210に出力する。

【0069】要求署名生成部210は、この第1の要求

(1, 199901081010, 199901081015, http://server300/object310?a=1)

【0073】[数2]で示した4項組は、シリアル番号が1、要求の発行日時が世界時で1999年1月8日10時10分、要求の有効期限が1999年1月8日10時15分、要求パラメータが"http://server300/object310/?a=1"であることを示している。

【0074】要求署名生成部210は、さらに、この第1の4項組に対してメッセージ・ダイジェスト関数を適用し、クライアント中継部200が持つ公開鍵暗号系の秘密鍵secretkey1を用いて、第1の電子署名

GET /object310?a=1 HTTP/1.1

Capability: (1, 199901081010, 199901081015, http://server300/object310?a=1)

Signature: signature1

【0078】他方、サーバ中継部300側の送受信部330は、第2の要求メッセージをネットワーク10経由で受信すると、これを要求メッセージ解析部350に出力する。

【0079】要求メッセージ解析部350は、以下の処理手順に従って、第2の要求メッセージを処理する。すなわち、

【0080】(1) 第2の要求メッセージを記録部320に送信する。記録部320は、これを保管し、クライアント100から要求を受け取った事実を後日客観的に証明可能とする。

【0081】(2) メッセージの先頭からサービス・オブジェクトの名前を抽出し、サーバ400の第1のリファレンスを取得する。

【0082】(3) HTTPにおけるリクエスト・ヘッダの形式のうち、"Capability"というフィールド名に対応する値を抽出し、第1のケイパビリティ

メッセージの中から要求パラメータとして"a=1"を抽出する。

【0070】次いで、要求署名生成部210は、メッセージ中に記されたサービス要求先"service1"に該当するURLを、URL対応表の中で検索する。URL対応表は、例えば記録部220が保管しており(図示しない)、該当するURLは"http://server300/object310"であるとする。このURLは、要求したサービス資源がホスト名"server300"であるサーバが所有するオブジェクト名"object310"という資源であることを示している。

【0071】要求署名生成部210は、(シリアル番号、発行日時、有効期限、要求パラメータ)からなる第1の4項組を生成する。この場合の4項組は[数2]の通りとなる。

【0072】

【数2】

を生成する。この第1の電子署名を、"signature1"とする。

【0075】次いで、要求署名生成部210は、要求パラメータと第1の4項組と署名"signature1"を送受信部230に出力する。

【0076】送受信部230は、第1の4項組と要求パラメータを元に、[数3]に示すような第2の要求メッセージを、ネットワーク10上に送信する。

【0077】

【数3】

とする。

【0083】(4) HTTPにおけるリクエスト・ヘッダの形式のうち、"Signature"というフィールド名に対応する値を抽出し、第1の電子署名signature1とする。

【0084】(5) 第1のケイパビリティの有効期限内か否かを検査する。期限内であれば、次ステップ(6)に進む。他方、期限が消滅していれば、当該ケイパビリティが無効である旨のメッセージを送受信部330に出力し、クライアント100に向けて送信する。

【0085】(6) 第1のケイパビリティが無効ケイパビリティ集合に既に登録されているか否かを検査する。無効ケイパビリティ集合の中になければ、次ステップ

(7)に進む。他方、当該ケイパビリティが無効ケイパビリティであれば、その旨のメッセージを送受信部330に出力し、クライアント100に向けて送信する。

【0086】(7) 要求メッセージ解析部350は、第

1の電子署名signature1が第1のケイパビリティの正しい署名であるか否かを検査する。該検査は、要求メッセージ解析部350が保持しているクライアント中継部200の公開鍵publickey1を用いて行なう。検査の結果、正しい署名であることが判明すれば、第1のケイパビリティを無効ケイパビリティ集合に追加して、要求の処理を続行する。他方、正しくない署名であれば、要求の処理を中止する。

【0087】なお、ケイパビリティとは、要求元が要求するオブジェクトに対するアクセス権限等を記述した情報のことである。ケイパビリティの詳細については、例えば本出願人に既に譲渡されている特願平10-266141号明細書を参照されたい。また、上述のステップ(6)及び(7)において、無効ケイパビリティ集合を用いるのは、同じケイパビリティが不正に再利用されるのを防止するためである。

【0088】要求メッセージは、次いで、サーバ400に送信される。これに対し、サーバ400は、図5に示すような文書1を作成したとする。図示の通り、応答文書1は例えばHTML形式のコードである。

【0089】サーバ中継部300は、文書1で構成される第1の応答メッセージをサーバ400から受け取ると、これを応答署名生成部310に渡す。

【0090】応答署名生成部310では、少なくとも要求メッセージに含まれる要求パラメータ(この例では“a=1”)と文書1とを連結した結果のメッセージ・ダイジェストに対して、サーバ中継部300が持つ秘密鍵secretkey2で暗号化を行ない、第2の電子署名“signature2”を生成する。そして、第2の電子署名signature2を含んだ第2の応答メッセージを送受信部330に出力する。送受信部330は、これをクライアント中継部200に送信する。

【0091】また、応答署名生成部310は、要求パラメータと文書1とタイム・スタンプを連結した結果のメッセージ・ダイジェストに対して暗号化を行なうことで、第2の応答メッセージを生成するようにしてもよい。

【0092】また、文字列を連結した後にメッセージ・ダイジェストを計算する処理を、以下のような連結を含まないメッセージ・ダイジェストの計算で置き換えてもよい。

【0093】1:メッセージ・ダイジェストを初期化する。

2:要求パラメータを用いてメッセージ・ダイジェストを更新する。

3:文書1を用いてメッセージ・ダイジェストを更新する。

4:タイム・スタンプを用いてメッセージ・ダイジェストを更新する。

5:メッセージ・ダイジェストの終了処理を行う。

【0094】クライアント中継部200の送受信部230は、第2の応答メッセージを受信すると、これを応答メッセージ解析部250に出力する。

【0095】応答メッセージ解析部250は、第2の応答メッセージとこれに添付された第2の電子署名“signature2”とを検証する。また、クライアント中継部200では、第2の電子署名“signature2”と第2の応答メッセージを記録部200に保存し、サーバ400からいかなる応答メッセージが戻されたかを後日客観的に証明できるようにする。

【0096】検証結果が正しい場合は、少なくとも要求メッセージと応答メッセージと現在時刻とを連結した結果のメッセージ・ダイジェストに対して秘密鍵secretkey1を用いて第3の電子署名“signature3”を生成する。あるいは、要求メッセージと応答メッセージと現在時刻の各々のメッセージ・ダイジェストを連結した結果のメッセージ・ダイジェストに対して秘密鍵secretkey1で第3の電子署名“signature3”を生成するようにしてもよい。そして、第3の電子署名“signature3”を含んだ受領メッセージをサーバ中継部300に送信する。

【0097】サーバ中継部300では、受信した受領メッセージを受領書解析部340に入力して解析及び検証する。

【0098】受領メッセージが正しい場合は、記録部320にこれを保存し、クライアント中継部200が応答メッセージを受領した事実を後日客観的に証明できるようにする。

【0099】他方、受領メッセージが正しくない場合は、受領拒否メッセージをクライアント中継部200に送信する。

【0100】《注釈》\*:公開鍵暗号方式は、一方の鍵で暗号化すると他方の鍵でしか復号化できないという性質を持つ2個の暗号鍵で構成される。通常、暗号鍵の所有者は一方の鍵を第三者に流布する「公開鍵」として用い、他方の鍵を所有者自身が秘密管理する「秘密鍵」として用いる。送信者は、受信者の公開鍵でデータを暗号化することにより、受信者しか解読できない暗号メールの状態で安全にデータ送信することができる。また、公開鍵暗号方式の他の用途は、所謂「デジタル署名」である。公開鍵の所有者は自身の秘密鍵でデータを暗号化する。暗号データの受信者は、送信者の公開鍵を以って暗号データを復元できることから、送信者本人からの受信データであることを認証することができる。

【0101】[追補]以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。

【0102】例えば、上述した「発明の実施の形態」では、HTTPプロトコルを利用した実施例を中心に説明

したが、本発明の要旨はHTTPプロトコルに限定されない。各データ通信端末（クライアント、クライアント中継部、サーバ中継部、サーバ）どうしが、HTTP、S-Http、FTP、CORBA、IIOP、JavaRMI、TCP、UDP等、他の任意の通信プロトコルを用いてメッセージ送受信する場合であっても、本発明を好適に適用することができることは言うまでもない。

【0103】要するに、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0104】

【発明の効果】以上詳記したように、本発明によれば、遠隔手続きの実行に関する履歴情報を客観的に証明することができる、優れた遠隔手続き呼び出し方式を提供することができる。

【0105】また、本発明によれば、クライアントがサービス要求を行なったこと、サーバがサービス要求に対して応答したこと、クライアントがサーバからのサービス応答を受け取ったことを客観的に証明することができる、優れた遠隔手続き呼び出し方式を提供することがで

きる。

【図面の簡単な説明】

【図1】 本発明の実施に供されるネットワーク・システム1の構成を模式的に示した図である。

【図2】 本発明の他の実施例に係るネットワーク・システム1の構成を模式的に示した図である。

【図3】 クライアント中継部200の構成を模式的に示した図である。

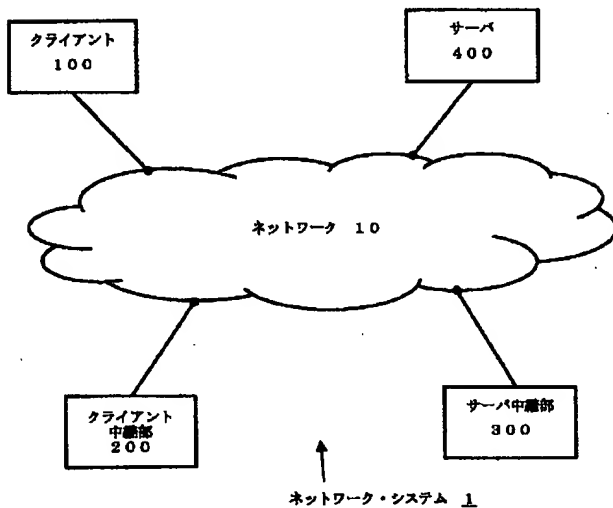
【図4】 サーバ中継部300の構成を模式的に示した図である。

【図5】 サーバ400が作成した応答メッセージの一例である。

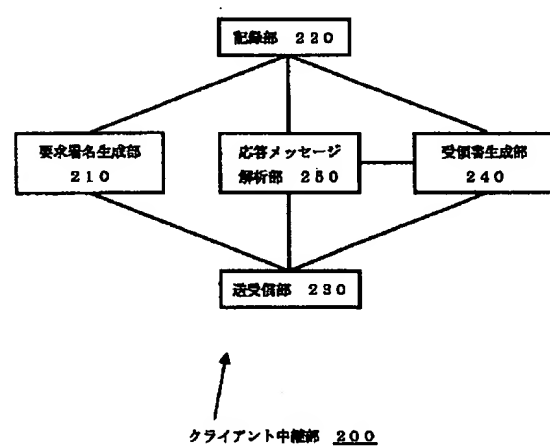
【符号の説明】

1…ネットワーク・システム、10…ネットワーク、100…クライアント、200…クライアント中継部、210…要求署名生成部、220…記録部、230…送受信部、240…受領書生成部、250…応答メッセージ解析部、300…サーバ中継部、310…応答署名生成部、320…記録部、330…送受信部、340…受領書解析部、350…要求メッセージ解析部、400…サーバ。

【図1】

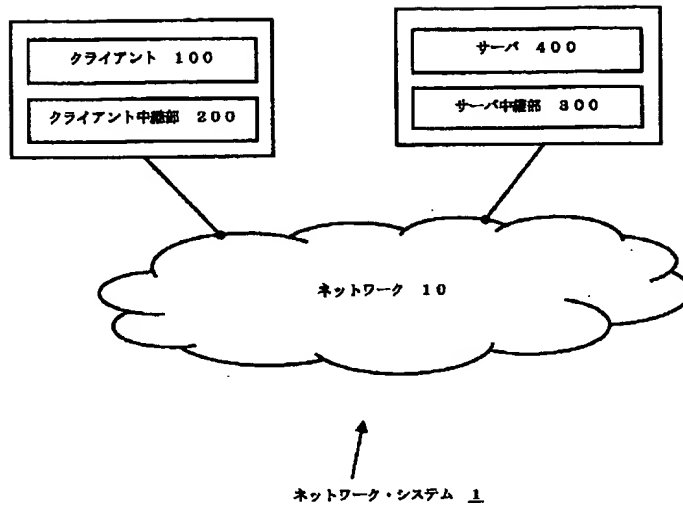


【図3】





【図 2】



【図 5】

```

<tr>
<td> aaa100
<td> 100
<td> 1000
<tr>
<td> aaa200
<td> 200
<td> 2000
<tr>
<td> aaa300
<td> 300
<td> 3000

```

【図 4】

